TMA Privacy Office Information Paper

Records Management • FOIA • DUAs • HIPAA Compliance • ADP Security • Privacy Act • System of Records • PIAs

Security Evaluation

HIPAA Security • November 2003

Standard Requirement

As a part of a covered entity's administrative safeguards, they must have a periodic technical and non-technical security evaluation that establishes the extent to which a covered entity's security policies and procedures meet the requirements of the security rule. According to the Security Rule, this evaluation is "based initially upon the standards implemented under this rule and subsequently, in response to environmental or operational changes affecting the security of electronic protected health information (EPHI)." This means that covered entities must assess how changes in the environment (e.g. security-related regulations and laws, new threats) and in their operations (e.g. changing mission, business practices, upgraded or new technology) will affect their compliance situation. The requirement for both "technical and non-technical" assessment indicates that the evaluation must include all organizational safeguards and systems, as well as a review of information systems. These security evaluations can either be performed by a covered entity's own workforce members or an outside organization, which would be acting as a business associate. This decision is left up to the covered entity. DHHS has not provided a definition for "periodic;" however, these evaluations can be done in conjunction with the risk analysis and risk management assessments that a covered entity must perform under the security management process standard.

See also:
45 CFR 164.308(a)(8)

Federal and DoD regulations that support this standard
OMB A-130 App. III
DoDR 5000.2
DoDI 5200.40
DoD 8510.1-M
DoDD 8500.1
DoDI 8500.2